

EXHIBIT B

Hunter @ NaptiBem.com



CORPORATION SERVICE COMPANY

Notice of Service of Process

WAS / ALL
Transmittal Number: 9561881
Date Processed: 02/02/2012

Primary Contact: Kathleen Delfine
Sterling & Sterling
135 Crossways Park Drive
Suite 300
Woodbury, NY 11797

Entity:	Sterling & Sterling, Inc. Entity ID Number 2284286
Entity Served:	Sterling & Sterling, Inc.
Title of Action:	Stratfor Enterprises, LLC vs. David Sterling
Document(s) Type:	Citation/Petition
Nature of Action:	Contract
Court/Agency:	Travis County District Court, Texas
Case/Reference No:	D-1-GN-12-000235
Jurisdiction Served:	Texas
Date Served on CSC:	02/01/2012
Answer or Appearance Due:	10:00 am Monday next following the expiration of 20 days after service
Originally Served On:	CSC
How Served:	Personal Service
Sender Information:	Bill Cobb 512-236-2326

Information contained on this transmittal form is for record keeping, notification and forwarding the attached document(s). It does not constitute a legal opinion. The recipient is responsible for interpreting the documents and taking appropriate action.

To avoid potential delay, please do not send your response to CSC
CSC is SAS70 Type II certified for its Litigation Management System.
2711 Centerville Road Wilmington, DE 19808 (888) 690-2882 | sop@cscinfo.com

C I T A T I O N
T H E S T A T E O F T E X A S
C A U S E N O . D - 1 - G N - 1 2 - 0 0 0 2 3 5

STRATFOR ENTERPRISES, LLC AND STRATEGIC FORECASTING, INC.

, Plaintiff

vs.

DAVID STERLING AND STERLING & STERLING, INC.

, Defendant

TO: STERLING & STERLING, INC.
BY SERVING ITS REGISTERED AGENT
CORPORATION SERVICE COMPANY
D/B/A CSC-LAWYERS INCORPORATING SERVICE COMPANY
211 7TH E. STREET, SUITE 620
AUSTIN, TEXAS 78701

Defendant, in the above styled and numbered cause:

YOU HAVE BEEN SUED. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10:00 A.M. on the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you.

Attached is a copy of the ORIGINAL PETITION of the PLAINTIFF in the above styled and numbered cause, which was filed on JANUARY 30, 2012 in the 353RD JUDICIAL DISTRICT COURT of Travis County, Austin, Texas.

ISSUED AND GIVEN UNDER MY HAND AND SEAL of said Court at office, February 01, 2012.

REQUESTED BY:
WILLIAM J. COBB, III
PO BOX 12548
AUSTIN, TX 78711--254
BUSINESS PHONE: (512) 375-0131
FAX: (512) 935-0545
bcobb@iw.com



Amalia Rodriguez-Mendoza
AMALIA RODRIGUEZ-MENDOZA
Travis County District Clerk
Travis County Courthouse
1000 Guadalupe, P.O. Box 679003 (78767)
Austin, TX 78701

PREPARED BY: LYDIA ANN MARTINEZ

----- 1st ----- February, 2012 ----- RETURN -----
Came to hand on the 1st day of February, 2012 at 2:30 o'clock P. and executed at
within the County of _____ on the _____ day
of _____, at _____ o'clock _____ M., by delivering to the within named
each in
person, a true copy of this citation together with the NOTICE OF NEW EFILE MANDATE ORDER AND THE LAWYER REFERRAL
SERVICE OF CENTRAL TEXAS accompanying pleading, having first attached such copy of such citation to such copy of
pleading and endorsed on such copy of citation the date of delivery.

Service Fee: \$ _____

Sheriff / Constable / Authorized Person

Sworn to and subscribed before me this the

By: _____

_____ day of _____

Printed Name of Server

Notary Public, THE STATE OF TEXAS

County, Texas

D-1-GN-12-000235

SERVICE FEE NOT PAID

P01 - 07356

☒ Original

☐ Service Copy

DELIVERED:

ON: 2/18/12
BY: [Signature] SCH 735
@: _____ am pm

CAUSE NO. D-1-GN-12-000235

STRATFOR ENTERPRISES, LLC and
STRATEGIC FORECASTING, INC.

Plaintiffs,

v.

DAVID STERLING and
STERLING & STERLING, INC.

Defendants

§
§
§
§
§
§
§
§
§
§

IN THE DISTRICT COURT OF

TRAVIS COUNTY, TEXAS

353RD JUDICIAL DISTRICT

PLAINTIFFS' ORIGINAL PETITION

Plaintiffs Stratfor Enterprises, LLC and Strategic Forecasting, Inc. file this Original Petition against Defendants David Sterling and Sterling & Sterling, Inc. and for cause of action would show the following:

I. DISCOVERY CONTROL PLAN

1. Plaintiff intends to conduct discovery under TEX. R. Civ. P. 190 Level 1.

II. PARTIES

2. Plaintiff Stratfor Enterprises, LLC is a Delaware limited liability company duly authorized to do business in Texas and with its principal place of business in Austin, Texas.
3. Plaintiff Strategic Forecasting, Inc. is a Delaware corporation duly authorized to do business in Texas and with its principal place of business in Austin, Texas.
4. Defendant David Sterling is a citizen of New York who may be served at his principal place of business at 135 Crossways Park Drive, Suite 300, Woodbury, NY 11797.
5. Defendant Sterling & Sterling, Inc. is a New York corporation which may be served at its principal place of business at 135 Crossways Park Drive, Suite 300, Woodbury, NY 11797, or through its Registered Agent for service of process: Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas, 78701.

III. JURISDICTION & VENUE

A. SUBJECT MATTER JURISDICTION

6. This Court has subject matter jurisdiction in that the amount in controversy is within the jurisdictional limits of this Court.

7. Additionally, this Court has subject matter jurisdiction under TEX. CIV. PRAC. & REM. CODE § 37.003 to declare the rights, status, and other legal relations of the parties whether or not further relief is or could be claimed.

B. PERSONAL JURISDICTION

1. DEFENDANT DAVID STERLING

8. This Court has personal jurisdiction over Defendant David Sterling because he purposefully availed himself of the privileges and benefits of conducting business in Texas by contracting with Plaintiff—who is duly authorized to and is doing business in Texas—through Plaintiffs' web servers located in Austin, Texas. Further evidence of such purposeful availment is David Sterling's contract with Stratfor Enterprises, LLC, which includes a choice of law provision providing that the rights and obligations of the parties would be governed by Texas law.

9. Additionally, this Court has personal jurisdiction over Defendant David Sterling because he purposefully availed himself of the privileges and benefits of conducting business in Texas and his contacts with Texas are continuing and systematic as evidenced by the fact that Mr. Sterling has obtained two (2) licenses from the Texas Department of Insurance to conduct the business of an Insurance Agent in Texas. The first, License ID 800998, first obtained in 1999, authorizes David Sterling to transact business in Texas as a General Lines Agent. The second, License ID 1290536, first obtained in 2004, authorizes David Sterling to transact business in Texas as a Surplus Lines Agent. Both licenses remain active, and expire on 9/15/2012 and 9/14/2012, respectively.

Mr. Sterling also holds over 65 active "appointments" by insurance companies. Each

appointment authorizes Mr. Sterling to conduct the business of insurance for a different insurance company in the State of Texas (e.g., United Healthcare of Texas, Foremost Llyods of Texas, Reliance Standard Life Insurance Company of Texas, etc.).

2. DEFENDANT STERLING & STERLING, INC.

10. This Court has personal jurisdiction over Defendant Sterling & Sterling, Inc. because it purposefully availed itself of the privileges and benefits of conducting business in Texas by registering to do business in Texas (Filing #800104604) in 2002; keeping that registration active each year thereafter (save a brief tax forfeiture) up to the present; paying franchise taxes in Texas (or receiving a waiver from the payment of them) from 2002 until the present; and appointing a Registered Agent for service of process in Texas.

C. VENUE

11. Venue is proper in this Court pursuant to TEX. CIV. PRAC. & REM. CODE §§ 15.002(1) and 15.002(4).

12. All or a substantial part of the events or omissions giving rise to this claim occurred in Austin, Travis County, Texas.

IV. BACKGROUND FACTS

13. Plaintiff Stratfor Enterprises, LLC ("Stratfor") is a subscription-based provider of geopolitical analysis. Stratfor publishes analysis via a subscribers-only website and customized email updates. Stratfor seeks to provide its paid subscribers a thorough understanding of international affairs, including what's happening, why it's happening, and what will happen next.

14. Stratfor is headquartered in—and its only place of business is in—Austin, Texas.

15. On December 6, 2011, Stratfor became aware that unidentified parties ("hackers") had illegally obtained email addresses, passwords, and credit card numbers of a large number of Stratfor Subscribers from Stratfor's website and/or its related servers. Subsequently, on

December 24, 2011, hackers destroyed a number of Stratfor servers and displayed a type of manifesto on Stratfor's website. Shortly thereafter, hackers publicly disclosed email addresses, passwords, and credit card numbers of certain Stratfor Subscribers.

16. Since December 7, 2011, Stratfor has been working closely with law enforcement officials at the Federal Bureau of Investigations ("FBI"), in an ongoing investigation regarding this "hacking." Furthermore, Stratfor has commissioned security consultants to investigate this serious privacy breach, and to prevent others from doing the same.

17. Specifically, in response to this hacking:

- Stratfor ensured, immediately on December 7, 2011, that all credit card companies were immediately notified by the FBI with the credit card numbers and subscriber names of all compromised cards. At the direction of the FBI, the credit card companies were not notified that Stratfor was associated with the compromised cards.
- At the request of the FBI, and in order to cooperate with the FBI's ongoing investigation, Stratfor did not publicly disclose that it knew it had been hacked and delayed notifying its Subscribers that their cards had been compromised.
- The hacking became public on December 24, 2011; thereafter, Stratfor notified its Subscribers on December 24, 25, and 28 that their cards had been compromised.
- Stratfor offered on December 28, 2011, at Stratfor's expense, identity protection services for paid Stratfor subscribers from CSID, a leading identity protection company.
- Stratfor commissioned SecTheory and Denim Group, leading Internet security firms, to work with it to rebuild its website, email system and internal infrastructure.
- Stratfor commissioned Rapid7, a leading internet security firm, to conduct external web application penetration assessments to further minimize the chance of subsequent successful hacks.
- Stratfor hired Verizon Business Network Services to conduct a forensic investigation of how and when the intrusions into Stratfor's systems occurred, in order both to understand what had happened and to be better able to prevent such intrusions in the future.
- Stratfor moved its entire e-commerce process to a PCI compliant third-party system, which eliminated the need for Stratfor to store any credit card information on its own servers.

- Stratfor enhanced the way it encrypts and stores passwords, and implemented new password requirements.

18. On January 20, 2012, Defendants David Sterling and Sterling & Sterling, Inc., filed a putative nationwide class action lawsuit on behalf of themselves and all others "whose financial and/or personal information was obtained by third-parties due to the breach of Stratfor's storage systems" against Strategic Forecasting, Inc. and George Friedman, its Chief Executive Officer.

19. The lawsuit was filed in the United States District Court for the Eastern District of New York, and will be referred to hereinafter as "the New York lawsuit," and is attached at Exhibit A.

20. The New York lawsuit does not name the "proper" party, Stratfor Enterprises, LLC, which is the party that was operating the business in question at the time the events alleged by Defendants in the New York Lawsuit occurred.

21. The first paragraph of the New York lawsuit recites: "This is a consumer class action for damages arising from Defendants' [Strategic Forecasting, Inc. and George Friedman] failure to secure its computer storage systems to protect Stratfor's users', subscribers', and those persons and entities that provided Stratfor with personal and financial information ("Customers"). Defendants also failed to timely notify Stratfor's Customers of their security breach until the unidentified third-parties who accessed Defendants computer storage systems notified the public on December 24, 2011."

22. The New York lawsuit alleges six causes of action: (1) Violation of the Federal Stored Communications Act, 18 U.S.C. § 2702; (2) Deceptive Acts and Practices Under New York General Business Law § 349; (3) False Advertising Under New York General Business Law § 350; (4) Breach of Contract; (5) Quasi-Contract or Implied-in-Law Contract; and (6) Negligence.

23. The last paragraph of the New York lawsuit requests class certification, appointment

of class counsel, more than \$50 million in compensatory damages, pre and post judgment interest, punitive damages, attorneys fees, and costs.

24. Strategic Forecasting, Inc., however, is not subject to personal jurisdiction in New York.

25. Strategic Forecasting, Inc., moreover, is not party to a current contract or relationship with Defendant David Sterling, and has never been party to any contract or relationship with Defendant Sterling & Sterling, Inc. Defendant David Sterling's current subscription began September 23, 2011, and is with Stratfor Enterprises, LLC.

26. As set forth in Exhibit B, Individual License Terms and Conditions (the contract between David Sterling and Plaintiff Stratfor Enterprises, LLC):

Notice: Effective August 1, 2011, Strategic Forecasting, Inc., in connection with a successful business transaction, changed the form in which it is doing business by assigning all of its assets and liabilities, including all Individual License Agreements, to Stratfor Enterprises, LLC, d/b/a Stratfor.

27. Like Strategic Forecasting, Inc. (the Defendant in the New York lawsuit), Plaintiff Stratfor Enterprises, LLC—the party with whom David Sterling *does* have a current contractual relationship—is not subject to personal jurisdiction in New York.

28. Plaintiffs deem it necessary to obtain a declaration of their respective “rights, status, and other legal relations,” in light of both the hacking described above and any uncertainty regarding their particular duties and obligations caused by the New York lawsuit.

29. In general, Plaintiffs seek a declaration of their contractual rights, duties, and obligations as set forth in Exhibit B, Individual License Terms and Conditions. Plaintiffs further seek a declaration of their respective statutory rights, duties, and obligations under the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*, attached at Exhibit C.

30. While Plaintiffs' right to obtain a declaratory judgment under Texas law and New York's inability to exercise jurisdiction over Stratfor Enterprises, LLC are sufficient cause for this

action to proceed in Texas, if further cause were necessary, the convenience of the parties and the ease of obtaining any relevant evidence is also served by proceeding in Texas.

31. In particular, Plaintiff Stratfor Enterprises, LLC is headquartered in Austin, Texas, and its Chief Executive Officer, George Friedman (named as a Defendant in the New York lawsuit) lives and works in Austin, Texas. The servers from which Stratfor provides its subscription service are located in Austin, Texas, and consequently, the hacking occurred in Austin, Texas. Defendant David Sterling contracted with Plaintiff Stratfor Enterprises, LLC, through its servers in located in Austin, Texas.

32. Defendants have a long history of continuous and systematic—and presumably convenient—contact with Austin, Texas. To wit, Defendant David Sterling has obtained and renewed his Insurance Agent License with the Texas Department of Insurance in Austin, Texas for the past 13 years, and Defendant Sterling & Sterling, Inc. has registered to do business and remitted franchise tax information to the Texas Secretary of State in Austin, Texas for the past 10 years.

V. CAUSES OF ACTION

A. DECLARATORY JUDGMENT

33. Plaintiff incorporates paragraphs 1 through 32 as if set forth herein.

34. “A court of record within its jurisdiction has power to declare rights, status, and other legal relations whether or not further relief is or could be claimed. An action or proceeding is not open to objection on the ground that a declaratory judgment or decree is prayed for. The declaration may be either affirmative or negative in form and effect, and the declaration has the force and effect of a final judgment or decree.” TEX. CIV. PRAC. & REM. CODE § 37.003(a), (b).

35. “A person interested under a deed, will, written contract, or other writings constituting a contract or whose rights, status, or other legal relations are affected by a statute, municipal ordinance, contract, or franchise may have determined any question of construction or

validity arising under the instrument, statute, ordinance, contract, or franchise and obtain a declaration of rights, status, or other legal relations thereunder." TEX. CIV. PRAC. & REM. CODE § 37.004(a). "A contract may be construed either before or after there has been a breach." TEX. CIV. PRAC. & REM. CODE § 37.004(b).

36. Plaintiffs seek a declaration of their respective rights, status, and legal obligations vis-à-vis Defendants as they concern the Stored Communications Act and their contractual relations, if any.

37. Effort has been made herein to seek declarations in the name of both Plaintiffs against both Defendants, where legally appropriate. Plaintiffs contend that Stratfor Enterprises, LLC (and not Strategic Forecasting, Inc.) has a contractual relationship with David Sterling (and not Sterling & Sterling, Inc.). The following requests for declaratory judgment should be interpreted accordingly.

1. CONTRACT – INDIVIDUAL LICENSE TERMS AND CONDITIONS

38. Plaintiffs seek a declaratory judgment that Defendant Sterling & Sterling, Inc. is a "corporation, enterprise, organization, or other commercial entity," and as such, Sterling & Sterling, Inc. was not an "Individual Licensee" of either of the Plaintiffs, as those terms are used in Exhibit B, Individual License Terms and Conditions.

39. Plaintiffs seek a declaratory judgment that Defendant Sterling & Sterling, Inc. is not party to an "Enterprise Licensee" with either Plaintiff, and thus, is not a party to any contract with either of the Plaintiffs, as that term is used in Exhibit B, Enterprise Database and Custom Portal License Terms and Conditions.

40. Plaintiffs seeks a declaratory judgment that *Stratfor Enterprises, LLC*, on the one hand, and *Defendant David Sterling, an individual*, on the other hand, are parties to a contract, as reflected in Exhibit B, Individual License Terms and Conditions. In other words—stated in the negative—Plaintiffs seek a declaratory judgment that (1) Strategic Forecasting, Inc. is not party to a

current contract with Defendant David Sterling, an individual, *or* with Sterling & Sterling, Inc.; and (2) that Stratfor Enterprises, LLC *and* Strategic Forecasting, Inc. are not parties to a contract, current or otherwise, with Defendant Sterling & Sterling, Inc.

41. Plaintiffs seek a declaratory judgment that they are not liable to Defendants "for any loss or injury caused in whole or in part by any error, delay or failure in procuring, compiling, interpreting, reporting, or delivering the service or content through the service" on or around December 24, 2011, or before, and thereafter, as those terms are used in Exhibit B, Individual License Terms and Conditions, Section 3. Disclaimer of Warranties and Limitation of Liability, and Enterprise Database and Custom Portal License Terms and Conditions, Section 3. Disclaimer of Warranties and Limitation of Liability.

42. Plaintiffs seek a declaratory judgment that any liability to Defendants "arising out of any kind of legal claim (whether in contract, tort, or otherwise), in any way connected with the service or the content available in the service shall not exceed the amount the individual licensee paid to Stratfor for use of the service," that is, \$349.00 with respect to Defendant David Sterling and \$0.00 with respect to Defendant Sterling & Sterling, Inc., as those terms are used in Exhibit B, Individual License Terms and Conditions, Section 3, and Enterprise Database and Custom Portal License Terms and Conditions, Section 3.

43. Plaintiffs seek a declaratory judgment that they did not contract with Defendants for "continuous" or "uninterrupted" Service; and, that Plaintiffs "shall not be liable to the Individual [or Enterprise] Licensee," due to any discontinuity, interruption, or the unavailability of its Service on or around December 24, 2011, or before, and thereafter, as those terms are used in Exhibit B, Individual License Terms and Conditions, Section 6. General, and Enterprise Database and Custom Portal License Terms and Conditions, Section 5. General.

2. STORED COMMUNICATIONS ACT.

44. Plaintiffs seek a declaratory judgment that they do not provide an "electronic communications service" to the public as that term is used in the Stored Communications Act, 18 U.S.C. § 2702(a)(1).

45. Plaintiffs seek a declaratory judgment that they do not provide "remote computing services" to the public as that term is used in the Stored Communications Act, 18 U.S.C. § 2702(a)(2), and defined at § 2711(2).

46. Plaintiffs seek a declaratory judgment that Defendants' credit card information and/or email address and password are "information pertaining to a subscriber or customer" as those terms are used in 18 U.S.C. § 2702(a)(3).

47. Plaintiffs seek a declaratory judgment that Defendants' credit card information and/or email address and password are not the "contents of communications" as that term is used in the Stored Communications Act, 18 U.S.C. § 2702(a), (c).

48. Plaintiffs seek a declaratory judgment that to the extent Defendants' "customer record" was divulged, it was divulged to a person other than a "governmental entity" as those terms are used in the Stored Communication Act, 18 U.S.C. § 2702(c)(6).

49. Plaintiffs seek a declaratory judgment that to the extent "information pertaining to" Defendants was divulged, it was divulged to a person other than a "governmental entity" as those terms are used in the Stored Communication Act, 18 U.S.C. § 2702(c)(6).

50. *If* the Court finds a violation of the Stored Communications Act, *then* Plaintiffs seek a declaratory judgment that they did not commit "the conduct constituting the violation" as those terms are used in 18 U.S.C. § 2707(a).

51. *If* the Court finds that either Plaintiff violated the Stored Communications Act, *then* Plaintiffs seek a declaratory judgment that "the conduct constituting the violation" was not "engaged

in with a knowing or intentional state of mind" as those terms are used in 18 U.S.C. § 2707(a).

52. If the Court finds that either Plaintiff violated the Stored Communications Act, *then* Plaintiffs seeks a declaratory judgment that "the violation" was not "willful or intentional" as those terms are used in 18 U.S.C. § 2707(c).

B. ATTORNEYS' FEES AND COSTS

53. Pleading further, if further pleading be necessary, and without waiving the foregoing, Plaintiffs request the following:

- A. Plaintiffs request that they be awarded their reasonable and necessary attorneys' fees pursuant to TEX. CIV. PRAC. & REM. CODE § 37.009 for having had to file and pursue this action.
- B. Plaintiffs also requests that they be awarded costs of suit pursuant TO TEX. CIV. PRAC. & REM. CODE § 37.009.

VI. CONDITIONS PRECEDENT

54. All conditions precedent to this action have been performed or have occurred.

VII. REQUEST FOR DISCLOSURE

55. Pursuant to Rule 194, you are requested to disclose, within fifty (50) days of service of this request, the information or material described in Rule 194.2(a) – (i).

PRAYER FOR RELIEF

Plaintiffs Stratfor Enterprises, LLC and Strategic Forecasting, Inc. respectfully request that Defendants David Sterling and Sterling & Sterling, Inc. be cited to appear, and answer, and that the Court grant the relief due Plaintiffs as follows:

- a. Declare the rights, duties, and obligations of Plaintiffs as set forth herein;
- b. Award Plaintiffs their reasonable and necessary attorneys' fees;
- c. Award Plaintiffs their costs of suit; and
- d. Award Plaintiffs all other relief, in law and in equity, to which Plaintiffs may be entitled.

DATED this 30th day of January, 2012.

Respectfully submitted,

JACKSON WALKER L.L.P.

By: /s/ Bill Cobb

Bill Cobb

Bar No. 00796372

100 Congress Avenue, Suite 1100

Austin, Texas 78701

(512) 236-2326

(512) 691-4446- Fax

**ATTORNEYS FOR PLAINTIFFS
STRATFOR ENTERPRISES, LLC and
STRATEGIC FORECASTING, INC.**

7916186v.1

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
DAVID STERLING, an Individual and
STERLING & STERLING, INC., a corporation on
behalf of themselves and others similarly situated,

Plaintiffs,

v.

STRATEGIC FORECASTING, INC. and GEORGE
FRIEDMAN

Defendants.
-----X

FILED
IN CLERK'S OFFICE
US DISTRICT COURT E.D.N.Y.

★ JAN 20 2012 ★

BROOKLYN
CIVIL ACTION NO. **CV12-297**

COMPLAINT

JURY TRIAL DEMANDED

CLERK'S OFFICE

LINDSEY A. J.

Plaintiffs DAVID STERLING ("Sterling") and STERLING & STERLING, INC. (hereinafter "S&S" or "Sterling & Sterling, Inc." and collectively, "Plaintiffs") bring this class action complaint on behalf of themselves and all others similarly situated (the "Class"), upon knowledge as to the facts and upon information and belief as to all other matters, based on the investigation of their counsel, NAPOLI BERN RIPKA SHKOLNIK, LLP, against defendants STRATEGIC FORECASTING, INC. ("Stratfor") and GEORGE FRIEDMAN (hereinafter "Friedman" and collectively with Stratfor, "Defendants") and state as follows:

I. Nature of the Action

1. This is a consumer class action for damages arising from Defendants' failure to secure its computer storage systems to protect Stratfor's users', subscribers', and those persons and entities that provided Stratfor with personal and financial information ("Customers"). Defendants also failed to timely notify Stratfor's Customers of their security breach until the unidentified third-parties who accessed Defendants computer storage systems notified the public on December 24, 2011.



2. Defendants keep and maintain a database of all Stratfor's Customers who provide Defendants with personal and financial information. Stratfor also maintains emails and communications they have with Customers on their servers. Stratfor did not encrypt or protect information provided by Customers to the company. Defendants' lax security measures allowed third-parties to access Defendants' computer storage systems at will and access any information desired.

3. In early December 2011, and on an exact date known only by Defendants, Defendants learned that a third-party, without authorization, obtained, disclosed, and utilized personal and financial information from Stratfor users and destroyed Stratfor's servers. Defendants kept their knowledge of the security breach secret from the public and did not alert its Customers until approximately December 28, 2011, and only after the third-parties had already disclosed to the public that they had succeeded in accessing Defendants' computer storage systems.

4. As a result of Defendants' failure to secure its systems and notify Plaintiffs and all members of the proposed Class of the theft of their personal and financial information, Plaintiffs and members of the proposed Class suffered and were caused injuries including: the financial expenses associated with third-party use of credit card and other financial information; the expense of securing replacements of compromised credit card numbers, online passwords, and the employment of monitoring services to protect against fraud; the deprivation of an opportunity to safeguard personal and financial information, monitor credit card activity, and take steps to prevent identity theft due to Defendants delayed notification to the public; exposure to computer viruses targeting corporations, individuals, and other entities using the email addresses and personal information obtained; embarrassment and invasion of privacy due public exposure of private email communications; loss of use of the Stratfor website that Plaintiffs and members of

the proposed Class paid subscription fees to access.

5. In this action, Plaintiffs seek to recover damages, equitable, and other relief available, from Defendants, on behalf of all Customers of Defendants' services.

II. Parties, Jurisdiction, and Venue

6. Plaintiff David Sterling is a citizen of the State of New York.

7. Plaintiff Sterling & Sterling Inc. is corporation existing and organized under the laws of the State of New York, whose principal place of business is 135 Crossways Park Drive, Suite 300, Woodbury, NY 11797 and whose business is in the insurance brokerage industry.

8. Defendant Strategic Forecasting, Inc. is a corporation existing and organized under the laws of the State of Texas whose principal place of business is 221 West 6th Street, Suite 400 Austin, TX 78701 and whose business is analyzing and publishing global news online to and via email to subscribers.

9. Defendant George Friedman is a U.S. citizen and Stratfor's Chief Executive Officer ("CEO").

10. Jurisdiction is proper in this Court pursuant to: a) 28 U.S.C. § 1331, because this case involves a federal question; and b) 28 U.S.C. § 1332(d), because this is a class action lawsuit in which the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and at least one member of the putative class is a citizen of the State of New York, hence a different state than that of the Defendants.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because Plaintiffs reside in this District and a substantial portion of the events and omissions giving rise to this action occurred in this District.

III. Factual Allegations Concerning Plaintiffs David Sterling and Sterling & Sterling

12. Plaintiff Sterling is the CEO of S&S and a Customer of Defendants' Stratfor publication. On December 28, 2011, Sterling received an email from Stratfor with the address: mail@response.stratfor.com. The email was sent to Sterling's S&S email account, the email address that Sterling had provided to Defendants. The email entitled "Important security information from STRATFOR," informed Sterling:

As we alerted you over the weekend, an unauthorized party illegally obtained and disclosed personally identifiable information and related credit card data of some of our members.

We deeply regret that this event has occurred, and we are working to prevent it from happening again.

Our highest concern is the impact that this has had on you, our loyal members and friends.

As a result and at our expense, we have taken measures to provide our members whose personally identifiable information may have been compromised with access to CSID, a leading provider of global identity protection and fraud detection solutions and technologies.

We have arranged to provide one year of CSID's coverage to you at no cost. Please take advantage of this service. To verify the authenticity of this email and our partnership with CSID, please view this video from our VP of Intelligence, Fred Burton.

In order to activate your Global ID Protector coverage, visit www.csid.com/stratfor to complete a SECURE sign up process.

This process begins by submitting your unique PIN code: [Code omitted]

As part of our ongoing investigation, we have also decided to delay the launching of our website until a thorough review and adjustment by outside experts can be completed.

We expect this to take approximately a week, but it might take longer – please bear with us as we recover from this unfortunate event.

In the meantime, we will not be deterred from doing what we do best: providing our customers with top-notch geopolitical analysis.

Therefore, while our website is being tested we will be sending geopolitical

analysis to our members via email. If you do not wish to have our analytical content emailed to you, click the link at the bottom of this email to manage your email preferences.

Sincerely,
George Friedman

13. Sterling was also notified that his account with Amazon, a leading retailer website, had fallen victim to identity theft. An unidentified third-party had used his personal information obtained from Stratfor's security breach in order to create a false account with Amazon that posed as Sterling's account. In order to prevent further attempts by third-parties seeking to use Sterling's identity for unauthorized purposes, Sterling changed his passwords and accounts with online businesses, forums, and other entities.

14. In addition, after the security breach, the unidentified third-party began using Sterling's American Express credit card to Sterling's detriment.

15. Plaintiff Sterling & Sterling, Inc. is a subscriber to Defendants' Stratfor publication. The credit card information and email address stolen during the security breach are S&S's property.

IV. Factual Allegations

16. Stratfor is a subscription-based provider of geopolitical analysis. Stratfor caters to individual and corporate subscribers providing analysis and commentary on international affairs. Unlike traditional news outlets, Stratfor claims to use unique, intelligence-based approaches to gathering information including a combination of open-source monitoring and a network of human intelligence sources. Stratfor analysts evaluate events with the objective of simplifying the complexity of international affairs for its targeted intelligent readership. Stratfor claims its reporting is unbiased and not intended to support any ideology.

17. Stratfor has grown its Customer base to nearly one millions content subscribers and

users. Stratfor's subscriber base includes individuals interested in politics and foreign affairs, corporations, government agencies, law enforcement, and military personnel. As a result, Stratfor has access to sensitive financial and personal information on individuals and entities of public interest.

18. In early December, Friedman claims to have received information that Stratfor's website had experienced a security breach. Third-parties were able to obtain Stratfor's Customer credit card information along with personal data. Thereafter, Friedman met with an FBI special agent, who was already aware of the security breach, and informed Friedman that the FBI was investigating the incident. As recounted in Friedman's public letters, the FBI also notified credit card companies of the security breach and provided the credit card companies with lists of compromised cards numbers.

19. Defendants failed to timely disclose to its Customers and the public, some of which sought to conduct business with Defendants after the security breach, that its computer storage systems had experienced a security breach, that it was known that Customers' credit card and other information was stolen, and that Stratfor had no security system in place to defend against current or future attempts by third-parties to access, obtain, and infiltrate its computer storage systems and its Customer's personal and financial information.

20. In a letter dated January 11, 2012, and entitled, "The Hack on Stratfor" Friedman described his "dilemma" in not informing Stratfor's Customers and the public of the security breach as follows:

From the beginning I faced a dilemma. I felt bound to protect our customers, who quickly had to be informed about the compromise of their privacy. I also felt bound to protect the investigation. That immediate problem was solved when the FBI told us it had informed the various credit card companies and had provided those companies with a list of compromised cards while omitting that it had come from us. Our customers were therefore protected, as the credit card companies knew the

credit cards and other information had been stolen and could act to protect the customers. We were not compelled to undermine the investigation.¹

21. Friedman and Stratfor had an obligation to inform its Customers and the public, some which continued to seek to conduct business with Defendants, of the breach of security. Instead Defendants assumed that its Customers' credit card information was secure due to the FBI's notification of credit card companies. Thus, Stratfor determined that its Customers and the public were not entitled to be informed of the security breach. Further, Defendants strategically decided to withhold knowledge of the breach to Customers and the public knowing that Stratfor's computer storage systems were not more secure than they had been when compromised and no party responsible had been caught. Moreover, Defendants understood that even if a Customers' credit card company notified the Customer of the misappropriation, the credit card company would be unable to tell the Customer the source of the breach, depriving the Customer of the ability to take further precautions.

22. Defendants' basis for withholding news of the security breach from Customers and the public was proven wrong when third-parties again targeted Stratfor's computer storage systems. Friedman explained that:

Early in the afternoon of Dec. 24, I was informed that our website had been hacked again. The hackers published a triumphant note on our homepage saying that credit card information had been stolen, that a large amount of email had been taken, and that four of our servers had been effectively destroyed along with data and backups. We had expected they would announce the credit card theft. We were dismayed that emails had been taken. But our shock was at the destruction of our servers. This attack was clearly designed to silence us by destroying our records and the website, unlike most attacks by such groups.²

23. Because those who gained access to Stratfor's servers disclosed to the public that Stratfor's Customers' financial and personal information had been compromised, we will never

¹ <http://www.stratfor.com/weekly/hack-stratfor> (last visited Jan. 20, 2012).

² *Id.*

know when, if ever, Defendants would have disclosed the security breach.

24. Indeed, Defendants were strongly motivated to conceal the security breach due to their embarrassment at how easily their systems had been compromised due to the complete absence of security measures to protect such information. Friedman wrote in his letter, "We knew our reputation would be damaged by the revelation, all the more so because we had not encrypted the credit card files. This was a failure on our part."³

25. Friedman took full responsibility for the security failure and opined that the "failure originated in the rapid growth of the company. As it grew, the management team and administrative processes didn't grow with it."⁴

26. As a result of Defendants admitted failure to take reasonable steps to secure its payment processing systems, databases, and servers, third parties disclosed financial and personal information including, but not limited to, names, credit card numbers, credit card expiration dates, CVV number, username, passwords, email addresses, phone numbers, and addresses for an estimated 75,000 customers and 860,000 registered users who are now subject to, and have in fact been, used for identity theft, unauthorized credit card charges, and additional cyber-attacks. Amongst the information obtained by third-parties were 19,000 email addresses belonging to the U.S. government's .gov and .mil domains, at least 90,000 credit card accounts and 5.2 million private email communications subject to future disclosure. Information already disclosed and information expected to be leaked in the near future have and will lead to further invasion of privacy of class members, wrongful and malicious use of emails to assist in launching further attacks on the computer systems various entities and individuals alike.

27. In fact, Stratfor has admitted that its Customers have already fallen victim to

³ *Id.*

⁴ *Id.*

additional attempts by third parties to acquire more personal information on its Customers or infect their systems with computer viruses. In a January 6, 2012, email Defendants state:

While addressing matters related to the breach of Stratfor's data systems, the company has been made aware of false and misleading communications that have circulated within recent days. Specifically, there is a fraudulent email that appears to come from George.Friedman[at]Stratfor.com.

I want to assure everyone that this is not my email address and that any communication from this address is not from me. I also want to assure everyone that Stratfor would never ask customers and friends to provide personal information through the type of attachment that was part of the email at issue. This email, and all similar ones, are false and attempt to prey on the privacy concerns of customers and friends. We strongly discourage you from opening such attachments. We deeply regret the inconvenience this latest development has created.

While Stratfor works to reestablish its data systems and web presence, we ask everyone to please look for official communications, such as this one, and to monitor the Stratfor Facebook page and Twitter feed for company-approved communications.

28. The list of corporations and entities that have had private information taken and already disclosed include BAE Systems Plc, Boeing Co, Lockheed Martin Corp, Bank of America, Exxon Mobil Corp, Goldman Sachs & Co and Thomson Reuters. Several U.S. government-funded labs that conduct classified research in Oak Ridge, Tennessee; Idaho Falls, Idaho; and Sandia and Los Alamos, New Mexico are also included in Stratfor's database. Notable individuals who have had their private information disclosed publicly include, former U.S. Vice President Dan Quayle, former Secretary of State Henry Kissinger and former CIA Director Jim Woolsey.

V. Class Action Allegations

29. Plaintiffs bring this action on behalf of themselves and a Class consisting of all persons, corporations, or entities whose financial and/or personal information was obtained by third-parties due to the breach of Stratfor's computer storage systems. Excluded from the Class are Defendants and its affiliates, parents, subsidiaries, employees, officers, agents, and directors;

government entities or agencies, its affiliates, employees, officers, agents, and directors in their governmental capacities; a ny judicial officer presiding over this matter and the members of their immediate families and judicial staff.

30. Plaintiffs are members of the Class they seek to represent.

31. Upon information and belief, Defendants marketed and advertised to Customers that information provided to Defendants would remain confidential and private implying that reasonable security measures were in place to maintain confidentiality.

32. At all times relevant, Defendants misled Customers that the information provided to Defendants was protected and would remain confidential.

33. Upon information and belief, Plaintiffs and the Class relied upon the Defendants' promises to protect their confidential and private information.

34. Defendants' gross annual sales are approximately \$5-10 million. Defendants' sales revenues are believed to be generated through Customer payments to Stratfor.

35. Plaintiffs and the Class have been damaged as a result of Defendants' failure to secure its systems and notify Plaintiffs and the Class of the theft of their personal and financial information causing injuries including:

- a. direct financial expenses due to unauthorized use of credit card account information;
- b. hassle and expense of securing replacement of compromised credit card numbers, passwords, and employment of monitoring services to protect against fraud;
- c. the deprivation of opportunities to safeguard personal and financial information, monitor credit card activity, and take steps to prevent identity theft;
- d. losses as a result of computer viruses targeting corporations, individuals, and other entities using email addresses and personal information obtained;
- e. Potential disclosure of private email communications; and

- f. Loss of use of paid for services on the Stratfor website due to its being incapacitated for 18 days.

36. Defendants are liable to pay to Plaintiffs and the Class monetary, statutory, equitable, and consequential damages for Defendants foregoing acts as well as Plaintiffs' reasonable attorney's fees and costs of suit.

A. Numerosity - Federal Rule of Civil Procedure 23(a)(1)

37. At this time, Plaintiffs do not know the exact size of the Class; however, due to the nature of the trade and commerce involved, Plaintiffs believe that Class members number in the hundreds of thousands if not close to 1 million current and prior subscribers, users, and persons who provided Defendants with personal and financial information and are thus so numerous that joinder of all members is impracticable. The number of class members can be determined through appropriate discovery.

B. Typicality - Federal Rule of Civil Procedure 23(a)(3)

38. Plaintiffs' claims are typical of the claims of the Class because they and all of members of the Class have provided Defendants with personal and financial information and have been comparably injured through Defendants' misconduct as described above and were all subject to Stratfor's security breach.

C. Commonality - Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3)

39. There are numerous common questions of law and fact relative to Plaintiffs and the Class that predominate over any questions affecting Plaintiffs or individual Class members, including but not limited to the following:

- a. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard its Customers sensitive personal and financial information;

- b. Whether Defendants properly implemented security measures to protect Customer personal and financial information from unauthorized capture, dissemination, and misuse;
- c. Whether Defendants took reasonable measures to determine the extent of the security breach after it first learned of same;
- d. Whether Defendants' delay in informing Customers and the public of the security breach was unreasonable;
- e. Whether Defendants' method of informing Customers of the security breach and its description of the breach and potential exposure to damages as a result of same was unreasonable;
- f. Whether Defendants' conduct violates the Stored Communications Act, 18 U.S.C. § 2702;
- g. Whether Defendants' conduct violates the New York General Business Law §349 or §350;
- h. Whether Defendants' conduct constitutes negligence;
- i. Whether Defendants' conduct constitutes breach of contract; and
- j. Whether Defendants' conduct constitutes breach of a quasi-contract or an implied-in-law contract; and
- k. Whether Plaintiffs and the other members of the Class are entitled to damages or other equitable relief.

40. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

D. Adequacy of Representation - Federal Rule of Civil Procedure 23(a)(4)

41. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class.

42. Plaintiffs have no claims antagonistic to those of the Class.

43. Plaintiffs have retained competent and experienced counsel in complex class actions and consumer actions.

44. Counsel is committed to the vigorous prosecution of this action.

E. Insufficiency of Separate Actions - Federal Rule of Civil Procedure 23(b)(1)

45. Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual Customers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated Customers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendants.

F. Superiority - Federal Rule of Civil Procedure 23(b)(3)

46. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if the Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. Given the similar nature of the Class members' claims, class treatment of this litigation will ensure that all claims and claimants are before this

Court for consistent adjudication thereof and will be easily managed by the Court and the parties to this action.

VI. Claims Alleged

COUNT I

Violation of the Federal Stored
Communications Act, 18 U.S.C. § 2702

47. Plaintiffs incorporate each of the foregoing allegations as if fully set forth herein.

48. The Stored Communications Act ("SCA") provides consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S.Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, at 3557.

49. Section 2702(a)(2)(A) of the SCA provides "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

50. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

51. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

52. Defendants provide remote computing services to the public through online systems that accept user inputs for computer storage and processing services. Defendants store personal and financial information on behalf of the public and utilize such information to process its services on behalf of Customers.

53. Upon information and belief, by failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Defendants knowingly divulged customer names, credit card numbers, credit card expiration dates, CVV number, username, passwords, email addresses, emails, phone numbers, and addresses due to the security breach of their computer storage systems. Further, upon learning that their servers and computer storage systems had been intruded upon and information had been obtained and accessed by third-parties, Defendants failed to safeguard their systems, inform Customers or the public of the security breach, and continued to knowingly divulge Customers information to third-parties.

54. As a result of Defendants conduct described herein and its violations of the SCA, Plaintiffs and the other members of the Class have suffered injuries as described above.

55. Plaintiffs, on their own behalf and on behalf of the other members of the Class, seek judgment in their favor and against Defendants awarding them and the other Class members the maximum statutory damages available under 18 U.S.C. § 2707, including punitive damages for willful or intentional violations.

COUNT II

Deceptive Acts and Practices Under New York General Business Law §349

56. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

57. Upon information and belief, Defendants willfully or knowingly engaged in

deceptive and misleading representations and omissions aimed at deceiving reasonable consumers and the public that Defendants were taking reasonable steps to secure Customers' personal and financial information on their servers and computer storage systems.

58. Defendants advertised to Customers and the public that information submitted, transmitted, and inputted through Defendants' website would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

59. As a direct and proximate cause of Defendants' deception to Customers and the public, Plaintiffs and the Class have suffered and continue to suffer harm and damages as described in the foregoing.

60. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered and that are available at law.

COUNT III

False Advertising Under New York General Business Law §350

61. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

62. Upon information and belief, Defendants willfully or knowingly engaged in deceptive and misleading representations through false advertisement aimed at deceiving reasonable consumers and the public that Defendants were taking reasonable steps to secure Customers personal and financial information on their servers and computer storage systems.

63. Defendants advertised to Customers and the public that information submitted, transmitted, and inputted through Defendants' website would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

64. As a direct and proximate cause of Defendants' deception to Customers and the

public, Plaintiffs and the Class have suffered and continue to suffer harm and damages as described in the foregoing.

65. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered that are available at law.

COUNT IV

Breach of Contract

66. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

67. Defendants breached their contract with Plaintiffs and other members of the Class who entered into contracts and a paid subscription fee for Defendants publication and website services.

68. As a result of Defendants security failure, the destruction of Stratfor's servers left the website crippled for nearly three weeks from December 24, 2011 through January 11, 2012 leading to a loss of at least \$1.3 million in services Customers paid for but did not receive and thus deprived Plaintiffs and subscribing members of the Class the benefit of their bargain with Defendants due to the Stratfor's security failure.⁵

69. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered that are available at law.

COUNT V

Quasi-Contract or Implied-In-Law Contract

70. Plaintiffs incorporate the allegations within all prior paragraphs within this

⁵ This figure assumes a subscriber base of 75,000 customers, a stated retail price of \$349 annually, and a loss of service for 18 days.

Complaint as if they were fully set forth herein.

71. Defendants entered into a quasi-contract or alternatively an implied-in-law contract with Plaintiffs and members of the Class to take reasonable steps to protect, hold, and maintain personal and confidential information provided to Defendants.

72. Plaintiffs and members of the Class conferred a benefit upon Defendants by providing Defendants with personal and financial information so as to allow Defendants to contact, transmit billing information, advertise, promote, send email distributions, mail, and engage in commerce or solicit commercial transactions to further Defendants' business interests with respect to Plaintiffs and members of the Class.

73. Defendants impliedly and expressly through use and services provided accepted the corresponding obligation to protect, hold, and maintain personal and confidential information provided to Defendants by Plaintiffs and members of the Class.

74. As a result of Defendants security failure Plaintiffs and members of the Class suffered as a direct and proximate cause the damages described above. Defendants are liable to Plaintiffs and the Class for all just and equitable relief Plaintiffs and the Class suffered.

COUNT VI

Negligence

75. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

76. Defendants assumed a duty of care deriving from the nature of services provided, the catastrophic consequences of breach of security, and the nature of the relationship between Plaintiffs and Class members with Defendants. Thus, Defendants were required it to exercise reasonable care to secure and safeguard Plaintiffs' and members of Class' personal and financial

information by agreeing to accept Plaintiffs' and Class members' personal and financial information through its website and storing the information in its computer storage systems.

77. Defendants breached its duty of care by failing to provide reasonable security and by failing to protect Plaintiffs' and the other Class members' personal and financial data from being captured, accessed, disseminated, and misused by third parties.

78. Defendants also breached its duty of care by failing to provide accurate, prompt, and clear notification to Plaintiffs and members of the Class that their personal and financial data had been compromised by unauthorized third-parties.

79. As a direct and proximate result of Defendants failure to exercise reasonable care and use commercially reasonable security measures Defendants were the direct and proximate cause of Plaintiffs' and the other Class members' injuries as described above.


80. Plaintiffs and members of the Class have suffered injury in fact, including money damages, and will continue to incur damages as a result of Defendants negligence.

VII. Request for Relief

WHEREFORE, Plaintiffs request that this Honorable Court enter judgment in their favor and against Defendants and: (1) certify the Class set forth herein; (2) appoint Plaintiffs' Counsel as Class Counsel; (3) award compensatory damages in an amount greater than \$50 million; (4) award punitive damages in an amount to be determined at trial; (5) award pre-judgment interest and post-judgment interest on all compensatory and punitive damages; (6) award all costs, expenses and attorneys' fees incurred by Plaintiffs and the Class; and (7) award any and all other relief to which this Court deems Plaintiffs and the Class are justly entitled.

Dated: January 20, 2012
New York, New York

Respectfully submitted,
NAPOLI BERN RIPKA SHKOLNIK, LLP


HUNTER J. SHKOLNIK (HS4854)
ADAM J. GANA (AG1822)
350 Fifth Avenue, Suite 7413
New York, New York 10118
(212) 267-3700 (Phone)
(212) 587-0031 (Fax)
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
DAVID STERLING, an individual and
STERLING & STERLING, INC., a corporation on
behalf of themselves and others similarly situated,

CIVIL ACTION NO. _____

Plaintiffs,

COMPLAINT

v.

STRATEGIC FORECASTING, INC. and GEORGE
FRIEDMAN

JURY TRIAL DEMANDED

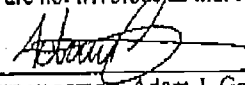
Defendants.

-----X

SUMMONS AND VERIFIED COMPLAINT

NAPOLI BERN RIPKA SHKOLNIK, LLP
Counsel for: Plaintiffs
350 Fifth Avenue, Suite 7413
New York, New York 10118
(212) 267-3700

The undersigned attorney hereby certifies, pursuant to Fed. R. Civ. P. 11 that I have read the within papers and that to the best of my knowledge and belief they are not frivolous as that term is defined in Fed. R. Civ. P. 11.


Attorney name: Adam J. Gana

PLEASE TAKE NOTICE:

☐ **NOTICE OF ENTRY**

that the within is a (certified) true copy of an _____ duly entered in the
office of the clerk of the within named court on _____ 200__.

☐ **NOTICE OF SETTLEMENT**

that an order _____ of which the within is a true copy, will be
presented for settlement to the HON. _____ one of the judges of the
within named Court, at _____ on _____ 200__ at _____ O'clock ____ M.

Dated, _____

Yours, etc.

Napoli Bern Ripka Shkolnik, LLP

Terms of Use

Individual License Terms and Conditions

- I. Access
- II. Intellectual Property Rights
- III. Disclaimer of Warranties and Limitation of Liability
- IV. Obligations of the Individual Licensee
- V. Renewal and Subscriber Cancellation
- VI. General
- VII. Privacy Policy

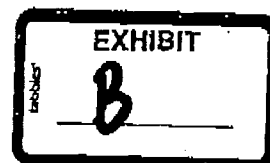
Enterprise Database and Custom Portal License Terms and Conditions

- I. Access
- II. Intellectual Property Rights
- III. Disclaimer of Warranties and Limitation of Liability
- IV. Obligations of Enterprise Licensee and the Custom Portal Licensee
- V. General
- VI. Privacy Policy

Individual License Terms and Conditions

The following are the terms and conditions (the "Terms and Conditions") for an Individual License, as defined below, to the information service accessed at www.stratfor.com (the "Service"), owned by Stratfor Enterprises, LLC, d/b/a Stratfor ("Stratfor"). Individuals who have entered into an agreement with Stratfor (the "Agreement") for a limited, nonexclusive right to use the Service solely in accordance with the Terms and Conditions shall possess an Individual License (such individuals are referred to as an "Individual Licensee"). By using the Service under an Individual License, the Individual Licensee agrees to the Terms and Conditions. Please read the Terms and Conditions carefully. Stratfor reserves the right to modify, update, or alter the Terms and Conditions without prior notice at any time. In the event of any conflict between the terms of the Agreement and the Terms and Conditions, the Terms and Conditions shall control. By using the Service after any change in the Terms and Conditions is posted on www.stratfor.com, the Individual Licensee agrees to be bound by all of the changes.

Notice: Effective August 1, 2011, Strategic Forecasting, Inc., in connection with a successful business transaction, changed the form in which it is doing business by assigning all of its assets and liabilities, including all Individual License Agreements, to



Stratfor Enterprises, LLC, d/b/a Stratfor. Control of the enterprise, and all of the employees engaged in it, remain the same as before the transaction.

Section 1. Access

1.1 Access to the Service and to the content, services, tools, web pages, e-mails, RSS feeds, software APIs, bulk data downloads, widget downloads, and other features of the Service, including images, text, illustrations, logos, audio, and video files (the "Content"), for the term set forth in the Agreement is for the Individual Licensee ONLY and may not be shared within the Individual Licensee's organization or otherwise except as expressly provided herein.

1.2 Corporations, enterprises, organizations or other commercial entities may not, directly or indirectly, hold an Individual License or have access to the Service.

1.3 Access to the Service and its Content by an Individual Licensees does not provide the right to access the Enterprise service or any Custom Portal or the content, services, tools, and other features of the Enterprise service or of any Custom Portal.

Section 2. Intellectual Property Rights

2.1 The Service and the Content, as well as the compilation (meaning the collection, arrangement, and assembly) of the Content and the Service, are the property of Stratfor and are protected by copyrights, trademarks, service marks, or other proprietary rights.

2.2 Stratfor TM is a proprietary mark of Stratfor. Stratfor's trademark may not be used in connection with any product or service that is not provided by Stratfor, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Stratfor.

Section 3. Disclaimer of Warranties and Limitation of Liability

STRATFOR AND ITS AFFILIATES, AGENTS, AND LICENSORS DO NOT MAKE ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF ACCURACY, COMPLETENESS, CURRENTNESS, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE CONTENT AVAILABLE THROUGH THE SERVICE, AND THE SERVICE ITSELF, ARE PROVIDED "AS IS." ALL CONDITIONS,

WARRANTIES, TERMS, REPRESENTATIONS, AND UNDERTAKINGS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, IN RESPECT OF THE CONTENT AVAILABLE THROUGH THE SERVICE, AND THE SERVICE ITSELF, ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED. NEITHER STRATFOR NOR ANY OF ITS AFFILIATES, AGENTS, OR LICENSORS SHALL BE LIABLE TO THE INDIVIDUAL LICENSEE OR TO ANYONE ELSE FOR ANY LOSS OR INJURY CAUSED IN WHOLE OR IN PART BY ANY ERROR, DELAY, OR FAILURE IN PROCURING, COMPILING, INTERPRETING, REPORTING, OR DELIVERING THE SERVICE OR CONTENT THROUGH THE SERVICE. IN NO EVENT WILL STRATFOR, ITS AFFILIATES, AGENTS, OR LICENSORS BE LIABLE TO THE INDIVIDUAL LICENSEE OR TO ANYONE ELSE FOR ANY DECISION MADE OR ACTION TAKEN BY THE INDIVIDUAL LICENSEE OR BY ANYONE ELSE IN RELIANCE ON THE CONTENT AVAILABLE THROUGH THE SERVICE, OR ON THE SERVICE ITSELF, OR FOR ANY CONSEQUENTIAL, SPECIAL, OR SIMILAR DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE INDIVIDUAL LICENSEE AGREES THAT THE LIABILITY OF STRATFOR, ITS AFFILIATES, AGENTS, AND LICENSORS, IF ANY, ARISING OUT OF ANY KIND OF LEGAL CLAIM (WHETHER IN CONTRACT, TORT, OR OTHERWISE), IN ANY WAY CONNECTED WITH THE SERVICE OR THE CONTENT AVAILABLE IN THE SERVICE SHALL NOT EXCEED THE AMOUNT THE INDIVIDUAL LICENSEE PAID TO STRATFOR FOR USE OF THE SERVICE.

Section 4. Obligations of the Individual Licensee

4.1 The Individual Licensee may not copy, reproduce, republish, upload, post, transmit, distribute, sell, publish, broadcast, circulate, data mine, or use any robot, spider, or other automatic device, or manual process, to monitor or copy, the Content, or exploit the Content or the Service commercially in any way, without the prior written consent of Stratfor, provided, however, the Individual Licensee may download or copy the Content for personal use only, provided that all copyright and other notices contained therein are maintained.

4.2 The Individual Licensee is responsible for providing complete and accurate account information. It is the sole responsibility of the Individual Licensee to report any changes to the Stratfor Account Manager immediately.

4.3 The Individual Licensee is responsible for the confidentiality and use of his user name and personal password. The responsibility of the Individual Licensee extends to all activity and use under his user name and password.

4.5 The Individual Licensee agrees to indemnify and hold harmless Stratfor and its affiliates, agents, officers, directors, and employees from and against any and all liability, loss, claims, damages, costs, and/or actions (including attorneys' fees) arising from the use by the Individual Licensee of the Service or of any Content accessed or received from the Service

Section 5. Renewal and Subscriber Cancellation

5.1 Individual Licenses are prepaid for the term set forth in the Agreement and may be paid by credit card only. Activation begins upon payment. Unless otherwise notified by Stratfor, your credit card account will be automatically charged 60 days prior to the expiration of the term of your subscription. At that time, your Individual License will be renewed at the then current rate, unless you notify us of your desire to cancel your Individual License at least thirty (30) days prior to the renewal date, or within thirty (30) days following your automatic renewal for any Individual License with at least an annual term.

5.2 To cancel your Individual License, you may call our Customer Services Department at 1-877-978-7284 from within the United States and Canada or at +1-512-744-4300, option 2 from outside the United States and Canada, or send an e-mail request with the subject line "Subscription Cancellation Request" to service@stratfor.com. Please be sure to provide your name, address, phone number, e-mail address, user name and password for authentication, and the reason you want to cancel. Cancellations are processed upon receipt of the cancellation request. Upon cancellation, all fees and charges are nonrefundable. However, if a user requests cancellation of an Individual License with at least an annual term within thirty (30) days following its automatic renewal date (see Section 5.1), such request will be honored.

Section 6. General

6.1 Stratfor reserves the right to monitor the use of the Service by the Individual to ensure the Individual Licensee is in compliance with the Terms and Conditions. Stratfor

may terminate or suspend an Individual License in its sole discretion upon any violation of the Terms and Conditions by the Individual Licensee.

6.2 The Service includes facts, views, opinions, and recommendations of individuals and organizations deemed of interest by Stratfor. Stratfor does not guarantee the accuracy, completeness, or timeliness of, or otherwise endorse, these views, opinions, or recommendations, give investment advice, or advocate the purchase or sale of any security or investment.

6.3 Stratfor reserves the right to modify the Service or its availability at any time with or without notice to the Individual Licensee. Stratfor shall not be liable to the Individual Licensee or to any third party should Stratfor exercise its right to modify the Service or its availability. Stratfor does not guarantee continuous, uninterrupted, or secure access to the Service.

6.4 The right of the Individual Licensee to access the Service, as permitted under these Terms and Conditions, is subject to the receipt by Stratfor of the payment of the Individual License fee as set forth in the Agreement. In the event of an early termination of the Individual License for any reason, Stratfor shall not be obligated to refund any portion of the Individual License fee.

6.5 The rights and obligations of the Individual Licensee under the Individual License are not assignable or transferable. If any provision of the Individual License is held to be invalid under applicable law, the remaining provisions will continue in full force and effect. The Individual License, all intellectual property issues, and the rights and obligations of Stratfor and the Individual Licensee shall be governed by the laws of the State of Texas, without regard to its conflicts of law provisions.

Section 7. Privacy Policy

Stratfor is committed to protecting the privacy of Individual Licensees. Information that Stratfor collects stays within Stratfor and any information distributed to third parties is reported in aggregate only. Stratfor does not give or sell information collected from Individual Licensees. For more information, please read the full text of our Privacy Policy at www.stratfor.com.

Enterprise Database and Custom Portal License Terms and Conditions

The following are the terms and conditions (the "Terms and Conditions") for an Enterprise Database License, as defined below, to the Enterprise Database information service accessed at www.stratfor.com (the "Service"), owned by Stratfor Enterprises, LLC, d/b/a Stratfor ("Stratfor").

The Terms and Conditions also apply to a Custom Portal License, as defined below, which provides access to the Service and to one or more custom designed portals (each a "Custom Portal") which can be accessed via a hyperlink located on www.stratfor.com.

Institutions which have entered into a legally binding written agreement with Stratfor (the Agreement) (i) for a limited, nonexclusive right to use the Service solely in accordance with the Terms and Conditions shall possess an Enterprise License (such institutions are referred to individually as an "Enterprise Licensee"), or (ii) for a limited, nonexclusive right to use the Service together with one or more Custom Portals shall possess an Enterprise License and a Custom Portal License (such institutions are referred to individually as a "Custom Portal Licensee"). (Enterprise Licenses and Custom Portal Licenses are referred to collectively as "Licenses" and individually as a "License," and Enterprise Licensees and Custom Portal Licensees are referred to collectively as "Licensees" and individually as a "Licensee"). By using the Service and/or by accessing a Custom Portal under a License, Licensees and each of their Authorized Users, as defined below, agree to the Terms and Conditions.

Please read the Terms and Conditions carefully. Stratfor reserves the right to modify, update, or alter the Terms and Conditions without prior notice at any time. In the event of any conflict between the terms of the Agreement and the Terms and Conditions, the Terms and Conditions shall control. By using the Service after any change in the Terms and Conditions is posted on www.stratfor.com, Licensees and each of their Authorized Users agree to be bound by all of the changes. Notice: Effective August 1, 2011, Strategic Forecasting, Inc., assigned all of its assets, including all Enterprise Database and Custom Portal License Agreements, to Stratfor Enterprises, LLC, d/b/a Stratfor. Control of the enterprise, and all of the employees engaged in it, remain the same as before the transaction.

Section 1. Access

1.1 The right to access the Service or a Custom Portal and to the content, services, tools, web pages, e-mails, RSS feeds, software APIs, bulk data downloads, and widget downloads, and other features of the Service or a Custom Portal, including images, text, illustrations, logos, audio, and video files (in the case of each of the Service and a Custom Portal, the "Content"), for the term set forth in the Agreement is limited to those individuals identified in the Agreement ("Authorized Users"), who are either identified in the Agreement by individual user names or shared user names ("Authorized User Names") or who have been given authorized access to a secure network maintained by the Licensee which can be identified by the IP network address or addresses owned and/or controlled by the Licensee identified in the Agreement ("Authorized IP Addresses") and which is only accessible to persons approved by the Licensee and whose identities are authenticated at the time of log in and whose online activity is subject to review and regulation by the Licensee (such secure networks may include proxy servers maintained and controlled by the Licensee). Authorized Users may access the Service only via Authorized User Names or Authorized IP Addresses.

1.2 Access to the Service or a Custom Portal and to its Content is for Authorized Users ONLY and may not be shared within the Licensee's organization or otherwise except as expressly provided herein.

1.3 Access to the Service and to its Content by an Enterprise Licensee and its Authorized Users does not provide the right to access any Custom Portal or the Content of any Custom Portal.

1.4 Access to a Custom Portal and its Content by a Custom Portal Licensee and its Authorized Users does not provide the right to access any other Custom Portals and their Content unless explicitly authorized in the Custom Portal Licensee's Agreement.

Section 2. Intellectual Property Rights

2.1 The Service and any Custom Portal, and the Content of the Service and of any Custom Portal, as well as the compilation (meaning the collection, arrangement, and assembly) of the Content of the Service and of any Custom Portal, are the property of Stratfor and are protected by copyrights, trademarks, service marks, or other proprietary rights, provided, however, that in the case of any Custom Portal Licensee, any logo of such Custom Portal Licensee shall be and remain the sole property of such Custom Portal Licensee.

2.2 Stratfor TM is a proprietary mark of Stratfor. Stratfor's trademark may not be used in connection with any product or service that is not provided by Stratfor, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Stratfor.

Section 3. Disclaimer of Warranties and Limitation of Liability

STRATFOR AND ITS AFFILIATES, AGENTS, AND LICENSORS DO NOT MAKE ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF ACCURACY, COMPLETENESS, CURRENTNESS, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE CONTENT AVAILABLE THROUGH THE SERVICE AND ANY CUSTOM PORTAL, AND THE SERVICE AND EACH CUSTOM PORTAL ITSELF, ARE PROVIDED "AS IS." ALL CONDITIONS, WARRANTIES, TERMS, REPRESENTATIONS, AND UNDERTAKINGS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, IN RESPECT OF THE CONTENT AVAILABLE THROUGH THE SERVICE AND ANY CUSTOM PORTAL, AND THE SERVICE AND EACH CUSTOM PORTAL ITSELF, ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED. NEITHER STRATFOR NOR ANY OF ITS AFFILIATES, AGENTS, OR LICENSORS SHALL BE LIABLE TO A LICENSEE, TO ITS AUTHORIZED USERS, OR TO ANYONE ELSE FOR ANY LOSS OR INJURY CAUSED IN WHOLE OR IN PART BY ANY ERROR, DELAY, OR FAILURE IN PROCURING, COMPILING, INTERPRETING, REPORTING, OR DELIVERING THE SERVICE OR ANY CUSTOM PORTAL OR CONTENT THROUGH THE SERVICE OR ANY CUSTOM PORTAL. IN NO EVENT WILL STRATFOR, ITS AFFILIATES, AGENTS, OR LICENSORS BE LIABLE TO A LICENSEE, TO ITS AUTHORIZED USERS, OR TO ANYONE ELSE FOR ANY DECISION MADE OR ACTION TAKEN BY THE LICENSEE, BY ITS AUTHORIZED USERS, OR BY ANYONE ELSE IN RELIANCE ON THE CONTENT AVAILABLE THROUGH THE SERVICE OR ANY CUSTOM PORTAL, OR ON THE SERVICE OR ANY CUSTOM PORTAL ITSELF, OR FOR ANY CONSEQUENTIAL, SPECIAL, OR SIMILAR DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH LICENSEE AGREES THAT THE LIABILITY OF STRATFOR, ITS AFFILIATES, AGENTS, AND LICENSORS, IF ANY, ARISING OUT OF ANY KIND OF LEGAL CLAIM (WHETHER IN CONTRACT, TORT, OR OTHERWISE), IN ANY WAY CONNECTED WITH THE SERVICE OR ANY CUSTOM PORTAL OR THE CONTENT AVAILABLE IN THE SERVICE OR IN ANY

CUSTOM PORTAL, SHALL NOT EXCEED THE AMOUNT THE LICENSEE PAID TO STRATFOR FOR USE OF THE SERVICE OR THE CUSTOM PORTAL, AS APPLICABLE.

Section 4. Obligations of Enterprise Licensee and the Custom Portal Licensee

4.1 The Licensees, and their Authorized Users, may not copy, reproduce, republish, upload, post, transmit, distribute, sell, publish, broadcast, circulate, data mine, or use any robot, spider, or other automatic device, or manual process, to monitor or copy, the Content of the Service or of any Custom Portal, or exploit the Service, any Custom Portal, or their Content commercially in any way, without the prior written consent of Stratfor, provided, however, the Authorized Users may download or copy the Content for personal use only, provided that all copyright and other notices contained therein are maintained.

4.2 The Licensees are each responsible for the compliance with the Terms and Conditions by their respective Authorized Users and shall inform Authorized Users of the restrictions and other provisions of the Terms and Conditions.

4.3 The Licensees are each responsible for providing complete and accurate account information. It is the sole responsibility of the Licensees to report any changes to the Stratfor Account Manager immediately.

4.4 The Licensees are each responsible for the confidentiality and use of their respective Authorized User Names and passwords. The responsibility of the Licensees extends to all activity and use under their respective Authorized User Names and passwords and/or IP network authentication access.

4.5 The Licensees each agree to indemnify and hold harmless Stratfor and its affiliates, agents, officers, directors, and employees from and against any and all liability, loss, claims, damages, costs, and/or actions (including attorneys' fees) arising from the use by the Licensees and their respective Authorized Users of the Service, any Custom Portal, or of any Content accessed or received from the Service or a Custom Portal.

Section 5. General

5.1 Stratfor reserves the right to monitor the use of the Service and any Custom Portal by the Licensees to ensure the Licensees are in compliance with the Terms and

Conditions. Stratfor may terminate or suspend a License in its sole discretion upon any violation of the Terms and Conditions by a Licensee, or by any of its Authorized Users.

5.2 The Service and Custom Portals include facts, views, opinions, and recommendations of individuals and organizations deemed of interest by Stratfor. Stratfor does not guarantee the accuracy, completeness, or timeliness of, or otherwise endorse, these views, opinions, or recommendations, give investment advice, or advocate the purchase or sale of any security or investment.

5.3 Stratfor reserves the right to modify the Service and any Custom Portal or their availability at any time with or without notice to Licensees. Stratfor shall not be liable to the Licensees, to their Authorized Users, or to any third party should Stratfor exercise its right to modify the Service, any Custom Portal, or their availability. Stratfor does not guarantee continuous, uninterrupted, or secure access to the Service or to any Custom Portal.

5.4 The right of the Licensees, and their Authorized Users, to access the Service and any Custom Portal, as permitted under these Terms and Conditions, is subject to the receipt by Stratfor of the payment of the Enterprise License fee or the Custom Portal License fee, as applicable, as set forth in the Agreement. In the event of an early termination of the Enterprise License or the Custom Portal License for any reason, Stratfor shall not be obligated to refund any portion of the Enterprise License fee or the Custom Portal License fee.

5.5 The rights and obligations of the Enterprise Licensee under the Enterprise License, and of the Custom Portal Licensee under the Custom Portal License, are not assignable or transferable. If any provision of the Enterprise License or the Custom Portal License is held to be invalid under applicable law, the remaining provisions will continue in full force and effect. The Enterprise License, the Custom Portal License, all intellectual property issues, and the rights and obligations of Stratfor, the Enterprise Licensee, the Custom Portal Licensee, and Authorized Users shall be governed by the laws of the State of Texas, without regard to its conflicts of law provisions.

Section 6. Privacy Policy

Stratfor is committed to protecting the privacy of Licensees and of Authorized Users. Information that Stratfor collects stays within Stratfor and any information distributed to

third parties is reported in aggregate only. Stratfor does not give or sell information collected from Licensees or from Authorized Users. For more information, please read the full text of our Privacy Policy at www.stratfor.com.

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs & Annos)

Part I. Crimes (Refs & Annos)

→ Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

→ § 2701. Unlawful access to stored communications

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.



→ § 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

[(C) Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

→ § 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communi-

cation, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2703 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or cus-

tioner is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number).

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

→ § 2704. Backup preservation

(a) Backup preservation.--(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of--

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider--

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges.--(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

→ § 2705. Delayed notice

(a) Delay of notification.--(1) A governmental entity acting under section 2703(b) of this title may--

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

→ § 2706. Cost reimbursement

(a) **Payment.**--Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) **Amount.**--The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) **Exception.**--The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

→ § 2707. Civil action

(a) **Cause of action.**--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) **Relief.**--In a civil action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) **Damages.**--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) **Administrative discipline.**--If a court or appropriate department or agency determines that the United States

or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) **Defense.**--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) **Limitation.**--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) **Improper disclosure.**--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

→ § 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

→ § 2709. Counterintelligence access to telephone toll and transactional records

(a) **Duty to provide.**--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) **Required certification.**--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to

which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States: and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure.--

(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) Libraries.--A library (as that term is defined in section 213(f) of the Library Services and Technology Act (20

U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

→ § 2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions.--For purposes of this section--

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video tape rental and sale records.--(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer--

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if--

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that

cannot be accommodated by any other means, if--

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil action.--(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages in an amount of \$2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally identifiable information.--Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of old records.--A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption.--The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

→ § 2711. Definitions for chapter

As used in this chapter--

- (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;
- (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;
- (3) the term "court of competent jurisdiction" includes--
 - (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--
 - (i) has jurisdiction over the offense being investigated;
 - (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
 - (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or
 - (B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and
- (4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

→ § 2712. Civil actions against the United States

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

- (1) actual damages, but not less than \$10,000, whichever amount is greater; and
- (2) litigation costs, reasonably incurred.

(b) Procedures.--(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency

to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried in the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) **Administrative discipline.**--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) **Exclusive remedy.**--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) **Stay of proceedings.**--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms "related criminal case" and "related investigation" mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

END OF DOCUMENT



Amalia Rodriguez-Mendoza

District Clerk, Travis County
Travis County Courthouse Complex
P. O. Box 679003
Austin, Texas 78767

Date: November 3, 2008

TO: All attorneys of record in cases pending in Travis County District Court

NOTICE OF ENTRY OF NEW E-FILE MANDATE ORDER

The 2008 Court Order Regarding E-filing is effective as of November 1, 2008. You can view this order by selecting the link near the top of the following web page:

http://www.co.travis.tx.us/district_clerk/default.asp

If you have not yet established an e-filing account, please refer to Texas Online's eFiling Main Information at:

<http://www.texasonline.com/portal/tqi/en/info>

We are asking that you establish your account as soon as possible, but a grace period through the end of the year has been implemented to allow you adequate time to make e-filing preparations.

If you have any questions regarding the e-filing process or the order's application to any of your pending cases, you may call 512-854-FILE (512-854-3453) for assistance.

Thank you.

A handwritten signature in black ink, reading "Amalia Rodriguez-Mendoza".

Amalia Rodriguez-Mendoza
Travis County District Clerk

Travis County District Clerk's Office
Civil Division

Administrative Offices
(512) 854-9737
Fax: 854-4744

Civil and Family Division
(512) 854-9457
Fax: 854-6610

Criminal Division
(512) 854-9420
Fax: 854-4566

Jury Office
(512) 854-4295
Fax: 854-4457

THE LAWYER REFERRAL SERVICE OF CENTRAL TEXAS
A Non-Profit Corporation

**IF YOU NEED A LAWYER
AND DON'T KNOW ONE,
THE LAWYER REFERRAL SERVICE
CAN HELP**

512-472-8303

866-303-8303 (toll free)

www.AustinLRS.com

Weekdays 8:00 am to 4:30 pm

\$20.00 for first half hour attorney consultation

**(free consultations for personal injury, malpractice, worker's compensation,
bankruptcy, and social security disability)**

**This service is certified as a lawyer referral service as required by the State of Texas
under Chapter 952, Occupations Code, Certificate No. 9303**

**SI USTED NECESITA EL CONSEJO DE UN
ABOGADO Y NO CONOCE A NINGUNO
PUEDE LLAMAR
A LA REFERENCIA DE ABOGADOS**

512-472-8303

866-303-8303 (llame gratis)

www.AustinLRS.com

Abierto de lunes a viernes de 8:00 am-4:30 pm

\$20.00 por la primera media hora de consulta con un abogado

**(la consulta es gratis si se trata de daño personal, negligencia,
indemnización al trabajador, bancarrota o por incapacidad del Seguro Social)**

**This service is certified as a lawyer referral service as required by the State of Texas
under Chapter 952, Occupations Code, Certificate No. 9303**